

he Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries.

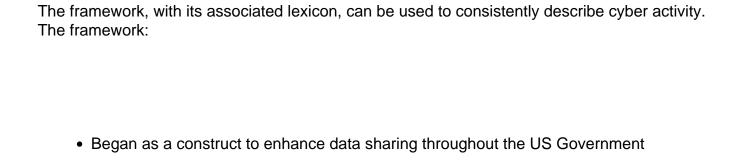
The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity.

The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber threat analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike.

HOW IT WORKS

The framework captures the adversary life cycle from PREPARATION of capabilities and targeting to initial ENGAGEMENT with the targets or temporary nonintrusive disruptions by the adversary, to establishing and expanding the PRESENCE on target networks, to the creation of EFFECTS and CONSEQUENCES from theft, manipulation, or disruption.

HOWTO USE THE FRAMEWORK



• Facilitates efficient situational analysis based on objective data

• Provides a simple, yet flexible, collaborative way of characterizing and categorizing

activity that supports analysis, senior level decision making, and cybersecurity

double-counting of threat data.

Offers a common backbone (cyber Esperanto) easier to map unique models to a
common standard that to each other
While the data that can be compiled using the framework can serve as useful points of information for analysis, the framework is not designed to serve as an analytic model. The frameworkerbitates அடிக்கு முற்ற முறையில் அவன்ற விறுவில் வரிக்கையில் முறிவர்கள் முறிவரிகள் முறிவர்கள் முறிவர்கள் முறிவர்கள் முறிவர்கள் முறிவர்கள் முறிவரிகள் முறிவரிகள் முறிவர
HOW THE FRAMEWORK WAS DEVELOPED
The idea of creating a cyber threat framework came from observations among the US policy community that cyber was being described by different agencies in a variety of ways that made consistent understanding difficult. There are over a dozen analytic models being used across

The framework will be scalable and facilitate data sharing at "machine speed." Implementation within the USG will include processes to reduce or eliminate



ADDITIONAL RESOURCES

- Cyber Threat Framework Overview | PDF
- Cyber Threat Framework How to Use Lesson Plan | PDF
- Cyber Threat Framework Lexicon | PDF

DNI-CTFHELP@dni.gov Submit Questions or Comments about Cyber Threat Framework



